UNITED STATES DISTRICT COURT
FOR DISTRICT OF NEW JERSEY

IQVIA INC. and IMS SOFTWARE SERVICES, LTD., *Plaintiffs,* v. VEEVA SYSTEMS, INC., *Defendant.*	Case No.: 19-cv- **COMPLAINT AND DEMAND FOR JURY TRIAL** ***Document Electronically Filed***

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs IQVIA Inc. and IMS Software Services, Ltd. (collectively, "IQVIA" or "Plaintiffs"), by and through their attorneys, as and for their Complaint against Defendant Veeva Systems, Inc. ("Veeva" or "Defendant"), allege as follows:

INTRODUCTION

1. Veeva has stolen IQVIA's valuable trade secrets, lied about the theft, breached contracts, brought baseless antitrust claims against IQVIA, and smeared IQVIA's name both in public and to the companies' shared customers. Despite all this, Veeva insists that the antitrust laws somehow require IQVIA to turn over its trade secrets to Veeva because Veeva wants to access and use them in connection with its data warehouse service, Veeva Nitro. Neither the antitrust laws nor common sense support Veeva's position, but that's not stopping Veeva. The company informed IQVIA that it intends to sue IQVIA to enforce its invented requirement. IQVIA therefore asks this Court for a declaratory judgment affirming that IQVIA is not required by the antitrust laws to turn over its valuable proprietary information and trade secrets to a direct competitor with a demonstrated track record of stealing these same trade secrets and smearing IQVIA's name.

2. IQVIA and Veeva both sell certain market research offerings that provide a variety of detailed information about healthcare professionals and organizations. Accurate information about healthcare professionals and organizations is crucial to life sciences companies, who rely on this market research to, among other things, market their products, distribute safety information, implement drug recalls, and recruit professionals for clinical trials.

3. IQVIA built these market research offerings ("IQVIA Healthcare Professional Data") over decades by spending millions of dollars each year to cultivate market research from thousands of sources and create comprehensive, accurate reports through the use of sophisticated technology, methodologies, processes, and considerable human effort. Veeva built its healthcare professional information products by theft.

4. To steal IQVIA's market research offerings, Veeva needed to access them. To begin, Veeva bought AdvantageMS, a small data services company, which itself had access to IQVIA market research offerings. Another major source of illicit access was Veeva's Master Data Management ("MDM") product. Life sciences companies use MDM products to process information obtained from various sources (including IQVIA) to ensure they have complete, consistent, and accurate information about healthcare professionals and organizations. Veeva's MDM software is cloud-based, meaning that allowing IQVIA Healthcare Professional Data into Veeva's MDM product involves placing IQVIA's closely-guarded trade secrets on the servers and in the hands of Veeva, a direct competitor for Healthcare Professional Data. Veeva designed its MDM product and its systems to facilitate theft of IQVIA market research offerings from mutual clients. Among other things, Veeva gave the employees building its competing healthcare professional data offering direct access to any IQVIA Healthcare Professional Data flowing into Veeva's MDM systems.

5. Veeva also stole IQVIA's Healthcare Professional Data through its "Data Report Card" marketing program. Veeva approached IQVIA customers and convinced them to grant Veeva access to IQVIA market research offerings in violation of IQVIA's license agreements with its customers. Veeva then compared these market research offerings to its own, ostensibly to show the customer that Veeva's competing product was a good substitute for IQVIA or other market research offerings that the life sciences company had already licensed. But Veeva did more than just run a biased comparison. The company used its access to IQVIA market research offerings to improve its own product by identifying and filling gaps in its own healthcare professional data offerings.

6. Veeva also used its illicit access to IQVIA's Healthcare Professional Data to improve other products. By Veeva's own admission, Veeva employees accessed IQVIA market research offerings when troubleshooting technical issues with Veeva software products. The employees that perform this technical support are often the same employees responsible for developing and updating Veeva's software products. These employees use their access to IQVIA market research offerings to design and test improvements to Veeva's software products that directly compete with offerings from IQVIA.

7. Veeva's theft of IQVIA's Healthcare Professional Data did not just violate federal and state trade secret statutes. It also violated dozens of contracts that IQVIA and Veeva entered into specifically to protect IQVIA market research offerings from misuse and theft. These contracts, called Third Party Access Agreements ("TPA Agreements"), granted Veeva limited access to IQVIA market research offerings but specifically forbade Veeva from using its access to IQVIA's intellectual property to improve Veeva's competing products. Veeva flagrantly violated these terms, lied about what it intended to do with its access to IQVIA market research offerings,

and actively encouraged mutual clients to breach related restrictions in IQVIA's licensing agreements with clients.

8. Veeva has also disparaged IQVIA in the marketplace, wrongfully accusing IQVIA of engaging in anticompetitive practices when IQVIA sought only to determine whether Veeva had adequate procedures in place to protect IQVIA's trade secrets before turning over its Healthcare Professional Data to Veeva.

9. In the fall of 2018, against the backdrop of its theft, disparagement, and disregard for its contractual obligations, Veeva sought TPA Agreements permitting IQVIA market research offerings to be loaded into Veeva's new data warehouse service, Veeva Nitro. A data warehouse is an information technology that exchanges data with one or more computer applications within a client organization to support analysis and reporting for that specific client organization.

10. IQVIA entered into two TPA Agreements permitting a very small amount of IQVIA's market research offerings to be used within Veeva Nitro. But, given Veeva's pervasive theft of IQVIA trade secrets, IQVIA has not granted additional licenses for Veeva Nitro. Instead of working to improve its lagging safeguards and controls and reform its culture of theft, and instead of coming clean about its past misconduct, Veeva has vowed to sue and seek both damages and an injunction requiring IQVIA to permit its intellectual property to be loaded into Veeva Nitro.

11. Even if Veeva did not have a history of stealing and misusing IQVIA's Healthcare Professional Data, nothing in the antitrust laws, or any other law, would require IQVIA to hand over to a direct competitor trade secrets it spent millions of dollars developing. In our free-market economy, companies can generally choose with whom they want to deal. But this basic principle applies with even greater force here, where Veeva's systematic theft, dishonesty, and deception

has given IQVIA no reason to trust Veeva and every reason to be concerned that Veeva will misuse any IQVIA market research information introduced into Veeva Nitro.

12. Because Veeva has told IQVIA that it intends to sue to force this access, however, IQVIA is entitled to a declaratory judgment affirming that it is not required to grant Veeva permission to host IQVIA market research products in Veeva Nitro or any other new Veeva software as a service ("SaaS") products. IQVIA therefore seeks a declaratory judgment that:

> IQVIA is not liable to Veeva based on any decisions not to enter into TPA Agreements permitting IQVIA's Market Research Offerings to be inputted into Veeva Nitro, or any later-introduced Veeva SaaS products, under any federal antitrust law, including Section 2 of the Sherman Act, or the laws of the states of New Jersey or California.

JURISDICTION AND VENUE

13. IQVIA brings this declaratory judgment action pursuant to 28 U.S.C. § 2201(a) to resolve an actual controversy between IQVIA and Veeva. The parties' dispute arises under Section 2 of the Sherman Act, 15 U.S.C. § 2, as well as state unfair competition and business tort laws. This Court has subject matter jurisdiction over the federal claims pursuant to 28 U.S.C. §§ 1331, 1337, 2201, and 2202. This Court has supplemental jurisdiction over the related state law claims under 28 U.S.C. § 1367.

14. IQVIA's dispute with Veeva is a ripe case or controversy. Veeva has indicated its intention to sue IQVIA regarding the matters described in this complaint by, among other things, sending IQVIA a set of claims that Veeva announced its intent to file. Accordingly, an actual case or controversy exists between the parties, and IQVIA need not wait for Veeva to file suit before it seeks a declaration from this Court.

15. Veeva is subject to personal jurisdiction in this district as Veeva is registered to conduct business within the State of New Jersey and has in fact conducted business in the state. Veeva also derives substantial revenue from services rendered within this district, and has

committed tortious acts within this district and/or has committed tortious acts which have caused injury within this district. Moreover, Veeva has continuous and systematic contacts within this district.

16. Venue is proper in this judicial district, pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2), as a substantial part of the events or omissions giving rise to the claim occurred in this district and Veeva resides in the district, pursuant to 28 U.S.C. § 1391(c)(2).

THE PARTIES

17. IQVIA Inc. is organized and existing under the laws of the State of Delaware with a principal place of business in Plymouth Meeting, Pennsylvania. IQVIA Inc. has offices at 100 IMS Drive, Parsippany, New Jersey, is registered under its predecessor name, IMS Health Incorporated, to conduct business within the State of New Jersey, and in fact conducts a significant portion of its business in this State and derives substantial revenue from services rendered within this district.

18. IMS Software Services is a corporation organized and existing under the laws of the State of Delaware with its registered office at 1209 Orange Street, Wilmington, Delaware, and holds the rights to certain intellectual property at issue in this case.

19. IQVIA, directly and through various subsidiaries around the world, provides, among other things, market research, analytics, technology and services to the life sciences, medical device, diagnostics and healthcare industries, to clients in over 100 countries. IQVIA's global reach allows IQVIA's life sciences clients to improve their understanding of, and interaction with, the global healthcare environment and in turn improve patient outcomes and save lives.

20. Since its founding more than sixty years ago, IQVIA has invested substantial sums to bring a wide range of innovative market research, analytics, technology and services offerings to the life sciences, medical device, diagnostics and healthcare industries. Through those years,

clients have realized substantial benefits from their use of IQVIA offerings. As a consequence, IQVIA has grown from a small business operating in two countries to a multi-billion dollar business employing approximately 60,000 people, operating in more than 100 countries.

21. Defendant Veeva is a publicly traded information and technology services company, organized and existing under the laws of the State of Delaware, with its principal place of business at 4280 Hacienda Drive, Pleasanton, California, and is registered to do business in the State of New Jersey.

22. IQVIA and Veeva are competitors.

FACTUAL ALLEGATIONS

I. IQVIA'S SUITE OF INNOVATIVE SERVICES TO IMPROVE HEALTHCARE AROUND THE WORLD

23. IQVIA is a provider of research, advanced analytics, and technology solutions to help life sciences companies and others develop new approaches to clinical development of medicines, speed innovation, and accelerate improvements in patient outcomes. Most relevant to this dispute are IQVIA's Market Research Offerings, Master Data Management software and services, Customer Relationship Management software and services, and Commercial Data Warehouse software and services.

A. IQVIA's Market Research Offerings

24. IQVIA offers various types of market research services ("Market Research Offerings"). One category of IQVIA Market Research Offerings is known as "Healthcare Professional Data" services, which span more than 100 distinct offerings localized in more than ninety countries. Another category of IQVIA Market Research Offerings is known as "Sub-National Information" services, which comprise multiple unique offerings in more than 50 countries and are described more fully below.

25. IQVIA invests hundreds of millions of dollars each year to build and improve one of the largest and most sophisticated information technology infrastructures in healthcare. IQVIA's infrastructure processes over 70 billion healthcare transactions from over 140,000 data suppliers annually to connect complex healthcare data while applying a wide range of privacy, security, operational, legal and contractual protections for data in response to local law, supplier requirements and industry leading practices in locations across the world. IQVIA Market Research Offerings are the product of the extensive skill and knowledge of IQVIA's experienced workforce who use IQVIA know-how, technology, processes and other proprietary intellectual property to create offerings unique to the communities that they serve.

26. IQVIA invests hundreds of millions of dollars annually to develop and maintain the information underlying its Market Research Offerings. IQVIA sources data, which does not contain any individual patient identifying information, from more than 140,000 data suppliers, covering approximately one million data feeds in countries around the world, including data from drug manufacturers, wholesalers, distributors, retail pharmacies, grocery stores, healthcare providers, government agencies and others. IQVIA also continuously invests in locating, recruiting and working with many sources of data, and developing and implementing innovative technologies and methodologies to apply to that data.

27. IQVIA also applies proprietary technology and know-how to edit, standardize, analyze and apply various statistical, processing and other methodologies to estimate or gather information relating to many aspects of healthcare practice in the real world, enabling IQVIA to produce syndicated or customized reports, audits and models, such as market forecasts and market intelligence, as well as other products and services.

1. Healthcare Professional Data

28. IQVIA's Healthcare Professional Data offerings synthesize information from tens of thousands of sources about healthcare professionals and healthcare organizations. For professionals, these records include names, phone numbers and addresses, as well as current license status, hospital and professional affiliations, primary and secondary specialties, certifications and other relevant information about their professional practices. IQVIA also collects and provides detailed information about the affiliations between healthcare organizations and healthcare professionals. IQVIA's practices regarding the collection, holding and processing of information about healthcare professionals vary to comply with applicable data protection laws.

29. IQVIA's Healthcare Professional Data offerings also synthesize and normalize information about healthcare organizations, which is acquired from tens of thousands of sources such as pharmacies, wholesalers, insurers, hospitals, integrated health networks, government agencies, medical associations and other organizations to provide comprehensive, timely reference information on hospitals, medical groups, long-term care facilities, outpatient surgery centers, imaging centers and home-health agencies.

30. IQVIA markets its Healthcare Professional Data under the OneKey® brand to life science clients, who use the market research to, *inter alia*, (i) market prescription medicines directly to physicians; (ii) share information with physicians about new medicines and newly approved uses for existing medicines, important label changes, safety warnings and changes in medical guidelines; (iii) distribute free samples; (iv) assist with drug recalls; (v) recruit healthcare practitioners for participation in clinical trials; (vi) comply with risk management program requirements; and (vii) conduct research in the public and private sectors, increasing the transparency of national, regional and local healthcare systems, improving health services and increasing efficiencies to lower costs.

31. Accurate and complete Healthcare Professional Data is vital to modern life sciences companies. For example, Veeva's own marketing materials state that the lost value and the opportunity cost of a 4% error rate in Healthcare Professional Data can cost a life sciences company tens of millions of dollars. According to Veeva, if just one out of every 25 sales calls is unsuccessful due to inaccurate or out-of-date healthcare professional data, a sales team of 300 representatives will waste $1.7 million in resources.

32. IQVIA has proprietary processes in place to develop and maintain the accuracy of its Healthcare Professional Data. IQVIA employs hundreds of research associates, called "data stewards," and data quality analysts who monitor thousands of data sources and resolve data conflicts for its Healthcare Professional Data. Among other tasks, these individuals process more than 1.5 million updates to IQVIA's Healthcare Professional Data per month globally, as well as perform scheduled maintenance, data investigations and complete client specific projects.

2. Sub-National Information

33. IQVIA's Sub-National Information provides an estimate of sales, dispensing, or prescribing of medicines at the regional, zip code and individual prescriber levels, with granularity varying based on local regulations and sources. There are two primary types of Sub-National Information services: sales information services, (*e.g.*, DDD™ information services) and prescription information services (*e.g.*, Xponent™ information services).

34. IQVIA carefully collects information used to create and develop its Sub-National Information offerings from a wide variety of data suppliers, including drug manufacturers, wholesalers, distributors, various types of pharmacies, hospitals, government and services organizations, group purchasing organizations, clinics, insurers, information technology vendors, and others in different formats and using different privacy-protecting techniques.

35. After collecting this information, IQVIA uses proprietary techniques to cleanse, bridge, edit and organize data, and applies sophisticated tools, including proprietary tolerances and business rules, to find and resolve quality issues in the data supplied to IQVIA. IQVIA also standardizes information for each transaction and links information received from suppliers to IQVIA reference files, which include physicians and other healthcare professionals, healthcare organizations, medicines, integrated health networks and market research classification schemes.

36. IQVIA employs additional quality control checks and processes in connection with maintaining applicable IQVIA databases, where the cleansed and standardized Sub-National Information is stored.

37. IQVIA then applies a combination of sophisticated computer processing, statistical sampling and projection methodologies, advanced analytics, forecasting methodologies and the skills and experience of its employees to create and deliver customized reports to clients through a variety of means, such as secure portals and direct delivery of data into client data warehouses.

38. IQVIA's life science clients use IQVIA's Sub-National Information offerings to understand real world healthcare practice, and with internal sales forces to set goals, determine resourcing, measure performance, calculate compensation and efficiently allocate company resources.

B. IQVIA Protects Its Market Research Offerings From Theft and Misuse

39. To protect the extensive skill, effort, and resources IQVIA applies to build and maintain its Market Research Offerings, IQVIA carefully guards these products from theft and misuse.

40. One vital form of protection for IQVIA's Market Research Offerings are the agreements that IQVIA customers sign as a condition of licensing these products. Among other

safeguards, these client licenses typically do not allow a client to share IQVIA Market Research Offerings with any third party.

41. IQVIA's life sciences clients sometimes use third-party vendors, including Veeva, to provide services related to or using the IQVIA Market Research Offerings licensed by the client. Since approximately 1992, IQVIA has implemented a Third Party Access ("TPA") program to permit clients to share access to limited portions of IQVIA's Market Research Offerings with vendors while maintaining reasonable protections for IQVIA's Market Research Offerings pursuant to TPA Agreements.

42. The purpose of IQVIA's TPA program is to protect the substantial investment IQVIA makes in its intellectual property, while at the same time accommodating client reliance on third-party vendors to analyze, process, and utilize information from IQVIA Market Research Offerings. Since 2011, IQVIA has entered into hundreds of TPA Agreements with Veeva, representing nearly 2,000 total licenses.

43. A TPA Agreement requires the vendor to acknowledge the confidential and proprietary nature of IQVIA Market Research Offerings. A TPA Agreement also restricts the vendor's use of IQVIA Market Research Offerings.

44. Among other provisions, IQVIA's TPA Agreements typically contain these terms and conditions:

(a) "No information may be used, directly or indirectly, to enhance, improve, update, validate, create, develop, benchmark or perform any similar service on any other [vendor] data, information, technology [or] methodology;"

(b) "No information may be used, directly or indirectly, to cleanse, correct, match, de-duplicate, or perform any similar service on any other [vendor] data, information, technology [or] methodology;"

(c) "Vendor may not download, print, copy, transfer or otherwise remove Information from Client's systems or local instance . . . except as necessary in order to make such Information available for use solely as part of Client's Application;"

(d) "Vendor may not hold any Information for common use for the benefit of two or more clients (including, for example, through the creation or maintenance of linkages or bridge files between Information and any other data);"

(e) "Access to the Information shall be restricted to employees of Vendor who need to access such information in connection with the Permitted Use set forth above in this [TPA Agreement] . . . In no event shall [IQVIA] Information be accessed by any employee or agent of Vendor with responsibilities involving the design or development of any of Vendor's (i) data sets or (ii) MDM Software . . . ."

45. Although the vast majority of client requests for TPA licenses for its preferred vendors are approved, IQVIA does not grant every TPA request it receives. IQVIA enters into a TPA Agreement where it is reasonably satisfied the confidential and proprietary IQVIA information to be licensed to the third party vendor will not be at unreasonable risk of misuse or misappropriation.

46. When IQVIA is asked to license information from an IQVIA Market Research Offering to a third party vendor that competes directly with the requested IQVIA Market Research Offering, IQVIA generally seeks written assurances that the third party will implement adequate safeguards and controls to avoid misuse and misappropriation of IQVIA intellectual property. In general, IQVIA receives adequate assurances, but on rare occasions, it does not and in those instances IQVIA will not enter into a TPA Agreement with a third party vendor until they provide those assurances.

47. In addition to its TPA program, IQVIA also protects its Market Research Offerings under applicable trademark, copyright, and trade secret laws. IQVIA also uses employment agreements, including non-disclosure agreements and confidentiality agreements, to protect against information flowing from current or former employees to third parties. IQVIA further employs technical restrictions to prevent the theft of data and intellectual property, including restrictions on the use of portable data storage devices.

C. IQVIA's Technology Offerings

48. Life sciences companies use a variety of software and technology products to access, organize, store, and process data. IQVIA markets three such products that are relevant to this suit: IQVIA Master Data Management ("MDM"), IQVIA Customer Relationship Management ("CRM"), and IQVIA Data Warehouse Services. Healthcare Professional Data and Sub-National Information are frequently used by life sciences companies within these applications.

1. Master Data Management (MDM)

49. An MDM Application refers to software developed to reconcile or link various records of demographic or other reference information relating to individuals, organizations, plans or products, which may have been obtained from different sources or at different times or pre-existing in a given database. An MDM Application is generally used to link information and records relating to an individual (*e.g.*, a physician) or an organization (*e.g.*, a hospital) to one client master file.

2. Customer Relationship Management (CRM)

50. A CRM Application is a computer-based application—whether installed on client computers, third-party hosted, or available through Software-as-a-Service ("SaaS")—that helps a sales force gather and organize information about its clients to help facilitate or improve relationships and interactions with each of those clients. Companies in the life sciences industry with sales forces generally use a CRM Application.

3. Data Warehouse Services and Products

51. Data Warehouse Services and Products exchange data from one or more applications within a client organization to support analysis and reporting (*e.g.*, business intelligence tools, decision support tools) for that specific client organization (*e.g.*, compared with a data mart or database associated with an application that is optimized for transaction processing).

II. VEEVA'S COMPETING PRODUCTS

52. Veeva competes with IQVIA. From its founding in 2007 until 2013, Veeva was basically a one-product company. Veeva sold a CRM software solution that it built on top of Salesforce.com's popular CRM product and modified for use by life sciences companies. Veeva's CRM product was a hit, and in 2013 the company launched a successful IPO.

53. Faced with the pressure of meeting rosy sales expectations included in its IPO prospectus, Veeva looked for shortcuts to expand into new markets. Veeva began offering its own MDM Application to life sciences companies in or around 2013. Called Veeva Network, Veeva's product aimed to combine MDM software with information regarding healthcare professionals and organizations. Veeva called this dataset, which directly competes with IQVIA's Healthcare Professional Data, "reference data" and marketed it under the brand name Veeva OpenData.

54. Veeva based its U.S. OpenData offering on a cheap, low-quality dataset developed by a company called AdvantageMS. AdvantageMS had access to IQVIA Market Research Offerings to build and develop its dataset. Veeva acquired AdvantageMS in June 2013.

55. Veeva repeated this strategy—acquiring low quality datasets and improving them through access to IQVIA Market Research Offerings—in countries around the world. Today, Veeva markets healthcare professional data offerings in approximately 46 countries.

56. In 2018, Veeva launched a data warehousing product called Veeva Nitro. As with Veeva's MDM and CRM products, Veeva Nitro is a cloud-based, SaaS product. This means that when customers sign up for Veeva Nitro, they agree to store their data—both self-generated and licensed by others—on servers controlled by Veeva.

III. VEEVA'S PATTERN OF THEFT AND DISPARAGEMENT

57. For years before Veeva requested permission to load IQVIA Market Research Offerings into Veeva Nitro, IQVIA believed that Veeva was misusing IQVIA's trade secrets to

improve Veeva's own competing products. These beliefs were well founded. Veeva's own statements, the results of an independent audit, and reports from the companies' shared customers all suggested that Veeva flouted its legal and contractual obligations to protect IQVIA's intellectual property. These red flags informed IQVIA's approach to TPA Agreements for Veeva Nitro.

A. Veeva's Statements and Actions Suggest a High Risk of Theft

58. Since it first entered the market for Healthcare Professional Data, Veeva's statements and actions strongly indicated that it was planning to build its offering on the back of IQVIA's substantial investments.

59. Veeva's started by trying to confuse the marketplace by infringing on IQVIA's trademarked brand name "OneKey." Veeva adopted the nearly identical name "OpenKey" for its competing product—adding only a single letter and mimicking OneKey's distinctive capitalization. Veeva changed course only after IQVIA sued to enforce its trademark, and rebranded its healthcare professional data product to "OpenData." Following the rebranding, IQVIA voluntarily dismissed the trademark infringement action.

60. Veeva's attempt to base OpenData on IQVIA's competing product ran far deeper than the name. From the beginning, Veeva stated that its reference data offerings would rely on "crowdsourcing" (also known as a "network effect") to improve Veeva's proprietary dataset based on data gathered from Veeva's customers. In fact, "crowdsourcing" was code for stealing confidential and proprietary information from IQVIA's Market Research Offerings. Many life sciences and other companies rely on IQVIA Healthcare Professional Data. Accordingly, when Veeva talked about getting data from a "crowd," that crowd was companies that had licensed IQVIA's Market Research Offerings. By proposing to take this information and convert it into

Veeva's proprietary dataset, Veeva was proposing wholesale theft of IQVIA's trade secrets in violation of IQVIA's licensing agreements with its customers and TPA Agreements.

61. Veeva eventually publicly claimed to back away from its crowdsourcing model, but the company's core strategy remained the same. In discussions with IQVIA, Veeva acknowledged that the joint design of Veeva's MDM Application and OpenData allowed healthcare professional data to flow from the client to OpenData. Because Veeva was targeting IQVIA Healthcare Professional Data customers for its MDM product, this design choice meant that OpenData would regularly incorporate IQVIA's intellectual property. Veeva could then turn around and market OpenData in direct competition with the IQVIA product Veeva had used to build its own product.

62. Veeva implemented little or no institutional separation between its MDM Application and OpenData. Employees of both operations were co-located within the same offices, data sat in the same technical and physical environment, and employees had responsibilities to both organizations. In fact, Veeva provided the employees building its OpenData product with direct access to any IQVIA Healthcare Professional Data that Veeva could get its hands on.

63. Veeva also admitted to accessing IQVIA Healthcare Professional Data and Sub-National Information in order to resolve technology issues reported by its CRM and MDM Application clients. A senior Veeva executive, in conversations with an IQVIA senior executive, explicitly admitted that the same Veeva CRM or MDM Application software engineers are responsible for both third line support functions and development and testing functions.

64. Veeva's strategy of competition through theft was also evident from lawsuits brought by other companies. By 2017, Veeva had been sued for similar conduct at least three times in less than five years. In 2013, Prolifiq, a software company, sued Veeva for patent

infringement and trade secret misappropriation after Veeva allegedly gained access to Prolifiq's trade secrets through a project for a mutual customer and then used this information to develop a competing product. *See Prolifiq Software Inc. v. Veeva Systems*, 13-cv-3644 (N.D. Cal. 2013). In 2017, Medidata, a clinical trial software services company, sued Veeva for trade secret misappropriation and unfair competition. Medidata alleged that Veeva poached several Medidata employees and induced them to steal trade secret information. *See Medidata Solutions, Inc. v. Veeva Systems*, 17-cv-589 (S.D.N.Y. 2017). Also in 2017, Sparta, another software company, sued Veeva and alleged that Veeva attempted to hire numerous Sparta employees in order to obtain confidential information to build a product that could compete with Sparta's products. *See Sparta Systems Inc. v. Veeva Systems*, cv-19-17 (N.J. Sup. Ct. 2017).

65. When IQVIA raised its concerns with Veeva, Veeva brushed them off. Veeva's CEO summed up the company's attitude in a 2016 email to IQVIA: "We are not talking about military secrets. We are talking about reference data."

B. An Independent Audit Confirms IQVIA's Fears and Reveals Veeva's Deceptions

66. Troubled by Veeva's disregard for IQVIA's rights to protect its valuable trade secrets, IQVIA engaged Veeva in a dialogue. In response, both publicly and privately, Veeva made several representations about technical and institutional safeguards built into its OpenData program. These purported safeguards included:

(1) Institutional separation between Veeva's MDM and OpenData teams: "The teams that compile and steward Veeva OpenData are not shared with any other groups, they do not influence the Veeva software products, and they do not have access to any Customer instance of Veeva [MDM] that would house [IQVIA] data."

(2) Technical protections against comingling of Veeva and IQVIA data: "Our technical solution (the Data Bridge) provides isolation at the country/customer level so that data access and [Data Change Request] processing of [IQVIA] data by Veeva's data teams is completely disabled . . . ."

(3) Auditability: "[IQVIA] Data IP is protected . . . [by t]wo party control (Veeva and Customer) so no single point of failure. Full audit trail."

67. Soon after Veeva made these statements, an independent audit by a leading global firm revealed that *all of them were false*. Veeva's purported protections were a sham.

68. IQVIA proposed an independent audit in September 2015. At first, Veeva agreed. Then, as the audit date approached, Veeva started backpedaling. Veeva deferred the start of the audit twice, before ultimately relenting in late October 2015.

69. Although Veeva bought itself more than a month to clean up its act, the audit revealed that Veeva lacked basic internal safeguards and controls to protect IQVIA's trade secrets from misuse. Even more troublingly, Veeva's representations to IQVIA and the marketplace were false.

70. The audit showed:

- There was no institutional separation between Veeva's MDM Application and OpenData. Contrary to Veeva's repeated assurances, the two products shared people, technology, and facilities.[1]
- Veeva had not implemented effective technical controls to separate IQVIA information in Veeva MDM from Veeva OpenData. The limited controls that did exist did not prevent the exporting and commingling of IQVIA Healthcare Professional Data.
- Veeva's MDM Application and OpenData were not effectively auditable. While Veeva represented that audits could be conducted to verify that sufficient safeguards and controls exist and prevent the misuse of IQVIA Healthcare Professional Data, or at the least detect misuse, Veeva's audit logs were so difficult to use and revealed such limited information that they were completely ineffective to prevent or detect misuse of IQVIA Healthcare Professional Data.
- Veeva had failed to effectively train its employees regarding Veeva's contractual and legal obligations surrounding IQVIA information. Despite

[1] Even the audit did not uncover the full extent of the direct access to IQVIA Healthcare Professional Data that Veeva had provided to the employees responsible for building OpenData because Veeva intentionally hid these facts from the auditors.

> signing TPA Agreements with IQVIA, Veeva did not adequately inform its employees about the TPA Agreement requirements regarding the handling and confidential nature of IQVIA's Market Research Offerings.

71. These conclusions were not IQVIA's alone. IQVIA engaged a leading digital security firm to review the audit, which confirmed IQVIA's concerns.

C. A Customer Reveals More Misuse

72. Veeva also ran biased analyses to compare IQVIA Healthcare Professional Data to Veeva OpenData in order to market and sell OpenData. These marketing comparisons were sometimes referred to as "Data Report Cards."

73. To prepare a Data Report Card, Veeva would compare an extract of health care professional information that a life sciences company had already licensed or otherwise obtained with Veeva OpenData. As Veeva well knew, for companies that had licensed IQVIA Healthcare Professional Data or IQVIA Sub-National Sales Information, Veeva's third-party use of IQVIA's trade secrets for this purpose violated both Veeva's TPA Agreements with IQVIA and IQVIA's licensing contracts with its customers. Veeva did it anyway.

74. In at least one instance, however, a client recognized that it had inadvertently sent identifiable IQVIA Healthcare Professional Data to Veeva for this marketing analysis. Although the client alerted IQVIA to the issue, Veeva took no steps to check for or notify IQVIA of the issue.

75. After the issue was uncovered, Veeva in-house counsel admitted that Veeva engaged in substantially similar unauthorized access of IQVIA Healthcare Professional Data on multiple occasions.

76. By performing scores of unlicensed comparisons, Veeva was able to secure illicit access to IQVIA's Market Research Offerings, which it could use to identify and improve gaps in Veeva OpenData. This insight provided a shortcut in the development process, because it was faster and cheaper for Veeva to focus only on updating the records it already knew were wrong.

77. Veeva understood that the client extracts may likely contain IQVIA Market Research Offering information and intentionally avoided asking clients whether the extract contained proprietary and confidential IQVIA Market Research Offering information. This approach allowed Veeva to maintain plausible deniability and avoided alerting the client to the need for a TPA Agreement, thereby keeping IQVIA in the dark.

D. Veeva's Disparagement of IQVIA

78. Veeva has also disparaged IQVIA in the marketplace, both publicly and in private communications, wrongfully accusing IQVIA of engaging in anticompetitive practices.

79. In or around 2015, Veeva sought to build a "consortium" of industry clients in an attempt to join forces to pressure IQVIA to commoditize its Reference Data Offering.

80. Veeva then filed antitrust counterclaims in an effort to smear IQVIA's reputation and unfairly generate business for its OpenData product.

81. Veeva wrongly asserted that IQVIA's choice not to grant certain TPA Agreement requests was anticompetitive even though IQVIA had granted Veeva dozens of TPA Agreements and had not issued certain TPA Agreements to Veeva in light of evidence of Veeva's disregard for IQVIA's intellectual property rights in its Market Research Offerings.

82. Veeva also wrongly accused IQVIA of, among other things, engaging in an unlawful conspiracy with Reltio, notwithstanding the fact that IQVIA's relationship with Reltio is nothing more than a non-exclusive arrangement that combines different offerings from two business partners to offer customers a superior offering than would exist without the partnership. Veeva is simply unhappy that it has to compete with the strong offering resulting from the non-exclusive partnership.

83. Veeva also wrongly accused IQVIA of conspiring with Cegedim, another provider of healthcare professional information at the time, simply because Cegedim had also expressed its

own concerns about allowing Veeva to license Cegedim's products for use within Veeva Network. Veeva continues to press its spurious allegations of a conspiracy even though both companies had their own independent concerns that Veeva would misuse their proprietary reference information—and for good reason, Veeva was in fact doing so.

84. In or around November 7, 2018, however, IQVIA was still evaluating the decision whether to license IQVIA Market Research Offerings within Veeva Nitro. Yet, Veeva's CEO, Peter Gassner, and Veeva's co-founder and President, Matt Wallach, sent an email to clients noting that "it . . . appears . . . that IQVIA is going to prohibit or severely limit the use of IQVIA reference data in Veeva's new Nitro data warehouse product," in an attempt to turn IQVIA's customers against IQVIA.

85. Veeva maintains a portion of its company website devoted to telling its customers that it is seeking to "Eliminat[e] Data Restrictions for Life Sciences" that are supposedly caused by IQVIA and that Veeva believes that "IQVIA's actions are arbitrary, anti-competitive and harm the industry."

86. Veeva's website does not, however, make any reference to Veeva's documented misappropriation of IQVIA's confidential and proprietary Market Research Offerings.

E. Veeva's Culture of Theft

87. Veeva has proven to have a culture of theft and dishonesty and has purposefully chosen to hide its trade secret theft from IQVIA.

88. In or around June 2013, Veeva purchased AdvantageMS, a small provider of healthcare professional information, to form the basis of Veeva's OpenData product in the United States. At the time of the acquisition, AdvantageMS had access to IQVIA Market Research Offerings, which access then became available to Veeva.

89. Veeva also misused and misappropriated IQVIA proprietary Market Research Offerings in connection with onboarding new OpenData clients and serving existing clients by making "data change requests" to inform and direct the research activities of Veeva data stewards to revise information in Veeva OpenData based on information learned from IQVIA's Healthcare Reference Offerings.

90. Veeva followed a similar roadmap in multiple other countries around the world, utilizing illicit access to IQVIA's proprietary Market Research Offerings to identify and fill gaps in its datasets, or sometimes to seed its datasets from the beginning. Veeva did this despite knowing, based on multiple discussions with IQVIA, that doing so violated restrictions in the client's licenses with IQVIA. This process allowed Veeva to shortcut the development process for its products by free-riding on IQVIA's efforts.

91. In addition to copying specific information from IQVIA's Market Research Offerings, Veeva also emulated IQVIA's proprietary architecture and classification detail for its market research information to gain an unfair advantage by leveraging IQVIA's years of research and development to find an optimal data architecture and classification structure that would be easy for clients to use and integrate with their systems.

92. Veeva never disclosed to IQVIA the various ways in which Veeva was unlawfully using IQVIA Market Research Offerings to improve Veeva OpenData. Instead, it chose to conceal that information from IQVIA and to make false denials and accusations to the marketplace.

IV. VEEVA SEEKS TO USE IQVIA MARKET RESEARCH OFFERINGS IN VEEVA NITRO

93. In the fall of 2018, IQVIA believed that Veeva was engaged in an ongoing campaign of wholesale data theft of IQVIA market research. As described above, the two companies were locked in litigation, and Veeva's disparagement campaign was in full force.

Against this backdrop, IQVIA received a handful of requests from customers for permission to load IQVIA Market Research Offerings into Veeva Nitro, Veeva's new data warehouse service.

94. IQVIA carefully considered these requests, and resolved them based on the risk they posed to IQVIA's closely-guarded trade secrets. On two occasions, IQVIA entered into TPA Agreements permitting a very small amount of IQVIA market research information to be loaded into Veeva Nitro. These requests both involved small amounts of IQVIA market research information.

95. The remaining Veeva Nitro TPA Agreement requests concerned a larger volume of IQVIA's Market Research Offerings, including IQVIA Healthcare Professional Data, the same product Veeva stole from IQVIA to build OpenData. Although it was wary of further theft, IQVIA did not flatly deny these requests. Instead, IQVIA sought to work with Veeva for the benefit of the companies' mutual customers.

96. IQVIA communicated with Veeva on multiple occasions describing its reasonable concerns and seeking to improve its understanding of Veeva Nitro to determine whether Veeva could be trusted to employ adequate safeguards and controls to protect IQVIA's Market Research Offerings from theft or misuse. However, Veeva's responses made it clear that IQVIA market research would be in serious jeopardy of theft and misuse. Unable to obtain reasonable assurances that Veeva would or could protect any IQVIA products loaded into Veeva Nitro from wholesale theft, IQVIA has not yet entered into TPA Agreements (beyond the two limited circumstances) to permit use of IQVIA Market Research Offerings in Veeva Nitro.

97. Rather than work openly and honestly to resolve IQVIA's concerns, Veeva chose to tell IQVIA that it would file a lawsuit. On June 1, 2019, counsel for Veeva sent counsel for IQVIA proposed Second Amended Counterclaims in the parties' ongoing suit. The Counterclaims

advance three new claims under Section 2 of the Sherman Act, all involving Veeva Nitro. In the first new claim, Veeva alleges that IQVIA has attempted to monopolize the market for "Life Sciences Data Warehouse Software." The second and third claims assert that IQVIA's TPA policy constitutes either a tying arrangement or impermissible exclusive dealing. Each of these claims are based on IQVIA's purported refusal to grant TPAs permitting its Market Research Offerings to be loaded into Veeva Nitro. Veeva only backed off from filing its amended counterclaims after the court expressed skepticism that these claims were timely within the contours of the existing litigation. But Veeva believes it can file the claims in a separate lawsuit.

98. Veeva's antitrust claims are baseless for several reasons. *First*, as explained above, IQVIA's TPA Agreement policy as a whole, and any choice to decline to issue certain TPA licenses relating to Veeva Nitro or other new Veeva SaaS products, is not predatory or anticompetitive. Rather, Veeva has a track record of stealing IQVIA's trade secrets and lying about it while smearing IQVIA's name, and nothing requires IQVIA to turn over its trade secrets to a company with such a history. IQVIA's TPA licensing decisions are motivated by its reasonable concern—fueled by *years* of misconduct by Veeva—that allowing Veeva access to IQVIA's Market Research Offerings will only lead to more theft. For the same reason, IQVIA's choice to not enter into certain TPA Agreements is not evidence of IQVIA's intent to monopolize any market.

99. To the contrary, IQVIA's TPA program is procompetitive. As courts and commentators routinely note, reasonable trade secret protections foster innovation and healthy competition. If IQVIA were unable to protect its substantial investment in Market Research Offerings from wholesale theft, it would have little incentive to build or maintain them. Nor would

any other company. Removing these reasonable protections would therefore deprive the market of these products.

100. *Second*, IQVIA does not have a dangerous probability of monopolizing the market for data warehouse services. The market for these services is highly competitive, and market leaders include IBM, Oracle, Google, Amazon, and many other technology organizations of all sizes. Compared with these behemoths, IQVIA's revenue for data warehouse services is modest, and far below the levels necessary to find a dangerous probability of monopolization. IQVIA therefore does not have a dangerous probability of monopolizing the data warehouse services market.

101. Veeva's claims for tying and exclusive dealing are similarly unfounded. IQVIA does not condition the purchase of its Market Research Offerings on either agreeing to purchase IQVIA's data warehouse services or agreeing to not purchase any other data warehouse services.

102. Nonetheless, with Veeva's claims written out and ready to serve, IQVIA is under a real and substantial threat that, at any moment, it could be brought into court to answer Veeva's baseless claims. IQVIA is therefore entitled to a declaration affirming that it is not liable to Veeva for taking reasonable steps to protect its trade secrets from further theft.

LEGAL CLAIMS

COUNT I

DECLARATORY JUDGMENT
(28 U.S.C. § 2201)

103. IQVIA alleges and incorporates the allegations of the paragraphs above as if fully set forth herein.

104. Veeva cannot establish that IQVIA is liable under the Sherman Act, any other federal antitrust law, or the laws of the states of New Jersey or California based on IQVIA's

commercial business decision not to license Veeva to use IQVIA's proprietary and commercially sensitive trade secrets within Veeva Nitro or other new Veeva SaaS offerings.

105. IQVIA is therefore entitled to a declaration that:

IQVIA is not liable to Veeva based on any decisions not to enter into TPA Agreements permitting IQVIA's Market Research Offerings to be inputted into Veeva Nitro, or any later-introduced Veeva SaaS products, under any federal antitrust law, including Section 2 of the Sherman Act, or the laws of the states of New Jersey or California.

PRAYER FOR RELIEF

WHEREFORE, IQVIA respectfully requests that the Court enter judgment in its favor and against Veeva on Count I granting a declaration pursuant to 28 U.S.C. § 2201 that :

(A) IQVIA is not liable to Veeva based on any decisions not to enter into TPA Agreements permitting IQVIA's Market Research Offerings to be inputted into Veeva Nitro, or any later-introduced Veeva SaaS products, under any federal antitrust law, including Section 2 of the Sherman Act, or the laws of the states of New Jersey or California;

(B) Costs of this suit; and

(C) Any such further relief as justice and equity may require.

DEMAND FOR TRIAL BY JURY

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs hereby demand a trial by jury.

Dated: July 17, 2019

Respectfully submitted,

CRITCHLEY, KINUM & DENOIA, LLC

By: */S/ MICHAEL CRITCHLEY*
Michael Critchley
Amy Luria

75 Livingston Avenue
Roseland, New Jersey 07068
Tel. (973) 422-9200
mcritchley@critchleylaw.com
aluria@critchleylaw.com

OF COUNSEL:

Steig D. Olson (*pro hac vice application forthcoming*)
Stephen A. Broome (*pro hac vice application forthcoming*)
Marlo A. Pecora (*pro hac vice application forthcoming*)
Sophia Qasir (*pro hac vice application forthcoming*)
David LeRay (*pro hac vice application forthcoming*)
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, New York 10010
Tel. (212) 849-7000
steigolson@quinnemanuel.com
stephenbroome@quinnemanuel.com
marlopecora@quinnemanuel.com
sophiaqasir@quinnemanuel.com
davidleray@quinnemanuel.com

Stephen A. Swedlow (*pro hac vice application forthcoming*)
Michelle Schmit (*pro hac vice application forthcoming*)
QUINN EMANUEL URQUHART & SULLIVAN, LLP
191 N. Wacker Drive, Suite 2700
Chicago, Illinois 60606
Tel. (312) 705-7400
stephenswedlow@quinnemanuel.com
michelleschmit@quinnemanuel.com

Attorneys for Plaintiffs IQVIA Inc. and IMS Software Services, Ltd.